PROFI
Wir entwickeln mehr als IT

Security and governance for Microsoft 365 Copilot

Protecting Copilot with Microsoft Purview

Microsoft Security



Generative AI introduces new threats

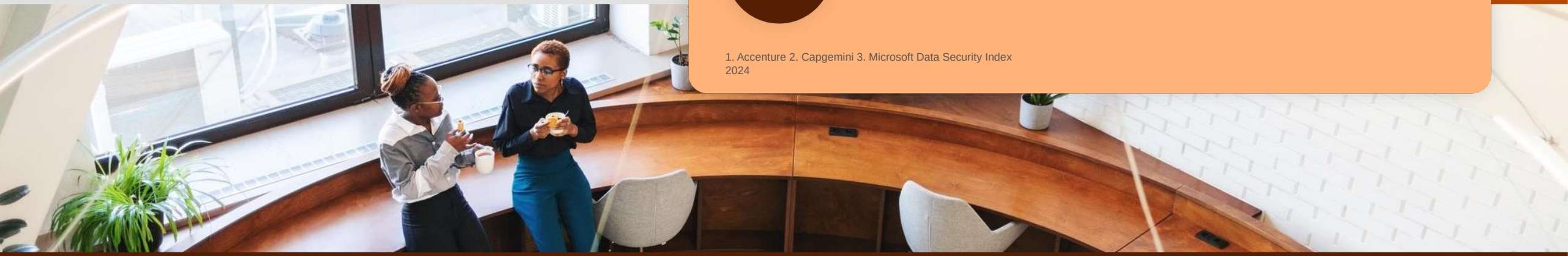
Generative AI is transforming the way we work, but it is also creating a continuously growing AI threat landscape with critical risk areas such as data leaks, new threats and vulnerabilities, and compliance violations. These threats amplify existing security risks such as data loss and insider risks. They also introduce new threats, such as prompt injection attacks and copyright infringement.

90% of organizations lack the tools to counter today's AI-powered threats.[1]

97% of organizations have experienced security breaches related to the use of generative AI.[2]

84% of all organizations lack confidence in managing data input into AI apps and tools.[3]

1. Accenture 2. Capgemini 3. Microsoft Data Security Index 2024



Microsoft 365 Copilot: AI with security by design

Customers trust Microsoft 365 Copilot with their sensitive data. Microsoft 365 is built on secure and responsible AI and offers industry-leading security and governance capabilities as well as tools to help organizations manage risk.

Microsoft 365 also offers a proven approach to privacy, built on a firm commitment to give you control over your data.

To manage and protect your Microsoft 365 Copilot data responsibly, you need to identify risky AI use quickly, for example when a user suddenly accesses a large amount of sensitive data. You also need insight into prompts and responses to ensure that you comply with your organization’s usage policies.



Minimizing risk as you scale Microsoft 365 Copilot

Microsoft 365 Copilot helps users create content based on their access permissions.

Minimizing risk means going beyond purely reactive oversight and establishing proactive governance. This ensures that the data powering Microsoft 365 Copilot is consistently managed, appropriately labeled, and properly protected.

Fully securing and governing Microsoft 365 Copilot requires the following:

Preventing data leaks and oversharing

Detect potential oversharing risks and get actionable recommendations on policies.

Identifying risky AI

Protect against data loss and insider risks with proactive alerts and adaptive protection.

AI governance and risk transparency

Help ensure that your use of Copilot and AI agents complies with legal requirements, corporate policies, and ethical principles.





A complete solution for securing and governing Microsoft 365 Copilot

Gain visibility into risks, enforce data protection, and apply governance controls with Microsoft Purview.

This comprehensive set of solutions helps your organization govern, protect, and manage Microsoft 365 Copilot data across your entire data estate. A unified view simplifies your data protection strategy, addresses data fragmentation, and ensures regulatory compliance.

How Microsoft Purview supports Microsoft 365 Copilot:

- Addresses information oversharing
- Protects against data loss and insider risks
- Governs AI use to comply with regulations and policies

Addressing information oversharing

Detect potential oversharing risks and get actionable policy recommendations.

Microsoft Purview helps you identify potentially overshared sites and files across your entire Microsoft 365 environment.

Get policy recommendations and apply them to minimize your specific oversharing risks. Remove organization-wide site access when needed. Get notified when new oversharing occurs, with options to remediate it.
Microsoft Purview protects sensitive files, regardless of where they are stored or transferred.



Key capabilities:

- Preventing processing of sensitive data
- Correcting overly broad permissions
- Overview of overshared content

Protection against data loss and insider risks

Analyze interactions with sensitive data, get alerts on risky activities, and adapt policies dynamically based on risk.

Microsoft Purview prevents data leaks by letting you view reports on sensitive data and unprotected files, receive alerts about risky usage, and detect when files contain sensitive data so that protection is applied automatically. You can protect files even when they are moved or downloaded. And with Microsoft Purview Insider Risk Management, you can restrict access for high-risk users.



Key capabilities:

- Alerts and reports on risky behavior and AI use
- Protecting sensitive files and interactions
- Dynamic application of security policies based on risky actions



Governing AI use to comply with regulations and policies

Help ensure that your use of Microsoft 365 Copilot complies with regulations such as the EU AI Act, organizational policies, and ethical principles.

Microsoft Purview helps you audit interactions with Microsoft 365 Copilot by giving you access to detailed log information. You can enforce retention and deletion policies for interactions as well as for meeting recordings and transcripts. You are also alerted when a potential compliance or ethics violation occurs, and you can open an investigation.

Key capabilities:

- Review of interaction content and audit logs
- Investigation of compliance and ethics violations
- Enforcement of lifecycle policies and legal retention periods

A complete solution for securing and governing Copilot



Microsoft Purview helps organizations adopt and scale Microsoft 365 Copilot and agents securely by detecting and preventing oversharing, preventing data loss, and enforcing governance aligned with evolving AI regulations.

"We use Microsoft Purview to ensure that content generated by Copilot is automatically classified and protected, so that only authorized users have access."

–Manjunatha Sivanna, IT Service Delivery Manager, Cummins



Greater security with PROFI AG

As a Microsoft partner, we are ready to help you defend your organization against cyberthreats. We have a strong security practice and the expertise you need to support you at every stage of your journey. We can assess your current environment, identify gaps, and help you implement and deploy the best possible security solutions tailored to your individual business needs.

- Secure Copilot adoption with clear governance
- Holistic approach to technology, security, and adoption
- Practical & tailored to your business

Your contact:

Jan Meyer-Böer
Head of Business Unit | Workplace Solutions | PROFI AG
Email: j.meyer-boeer@profi-ag.de
Phone: +49 511 676885-3028

Security for AI assessment | Microsoft 365 Copilot

Are you ready for Microsoft 365 Copilot?

Assess your security and governance readiness and get tailored recommendations to help you prepare your Microsoft 365 environment, identify risks, and protect and govern the use of Microsoft 365 Copilot.

Learn more



Resources

1. Using Microsoft Purview to manage data security and compliance for Microsoft 365 Copilot and Microsoft 365 Copilot Chat
2. Microsoft Purview protections for Copilot
3. Oversharing control at enterprise scale | Updates for Microsoft 365 Copilot with Microsoft Purview